Information Security Policy

Lizu Community network

JULY 2025

CERTIFICATION

By signing this document, I certify that I have read and reviewed the Lizu Community Network Information Security Policy – Version 1.0 - 2025, and I understand the contents completely. If I have any questions about these procedures or want to make any changes to suit my personal responsibilities, I will contact the Lizu Community Network team lead immediately.

Name (please print): _____

Signature: _____

Date: _____

Contents

1. Introduction

This top-level information security policy (ISP) governs the protection of information, which is one of Lizu Community Network's key assets and a critical component of the organization's overall information security management framework. This ISP outlines a set of guidelines to ensure that all staff adhere to the requirements regarding the security of digitally stored data. This security policy contains prescriptions specifically applicable to staff in terms of what they can do to improve the organization's overall security situation.

1.1. Purpose

The purpose of this policy is to establish a framework for managing risks and protecting Lizu Community Network's people and Information Resources (IR) against all types of threats, internal or external, intentional or unintentional. This document defines the security requirements for the proper and secure use of Information Technology services within the organization. Its goal is to protect Lizu and its users to the maximum extent possible against security threats that could jeopardize the integrity, confidentiality, availability, authenticity, and privacy of Lizu's information, systems, applications, and networks. This policy is intended to empower users to make decisions about their digital security needs, understand their specific risks, and know what to do or who to turn to for advice.

1.2. Scope

This document applies to all users in the organization, including temporary users, visitors with temporary access to services, and partners with limited or unlimited access time to services. Compliance with policies in this document is mandatory, and non-compliance will attract disciplinary actions, including suspension, restriction of access, or more severe penalties up to and including termination of employment or prosecution. Where illegal activities are suspected, Lizu may report such activities to applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions which will remain in force.

1.3. Version History

Version		Description/Summary of Revision	Date	Author
1.0		Initial version	04/07/2025	Digital Society of Africa

1.4. Responsibilities

Roles	Responsibilities
Executive Director	● Maintain, review and update policy **annually** from date above. Trust the team lead and appointed digital security champion to oversee process. **Policy can also be reviewed as and when necessary e.g following significant security incidents within and external to the organization - necessitating new policy definitions*
Executive Director	● Accountable for all aspects of the organization's information security.
Executive Director Digital Security Champion	● Responsible for the security of the IT infrastructure. ● Plans against security threats, vulnerabilities, and risks. ● Implements and maintain security policy documents. ● Plans for & ensures that regular staff security-training programs occur. ● Ensures that the IT infrastructure supports security policies. ● Responds to information security incidents. ● Helps in disaster recovery plans.
Information Owners	● Help with the security requirements for their specific area. ● Determine the privileges and access rights to the information resources within their areas.
Users/Staff	● Meet and abide by security policy requirements. ● Report any actual or attempted security breaches.

1.5. General Policy Definitions

This policy can only be activated through staff training to ensure everyone has the same understanding. Lizu should invest in regular staff security training as the IT space is constantly evolving. This policy will be distributed to all users electronically along with their employment contract, and each user signs to signal their understanding and willingness to comply with the policy and returns it to management. Any new staff will be given the policy as part of their orientation and onboarding process.

Any exceptions to the policies defined in any part of this document may only be authorized by the Executive Director. In those cases, specific procedures may be put in place to handle requests and authorization for exceptions. Every time a policy exception is invoked, there must be an entry into a security log specifying the date and time, description, reason for the exception, and how the risk was managed.

All IT services should be used in compliance with the technical and security requirements defined in the design of the services.

1. IT Assets Policy

1.1. Policy Definitions

- IT assets belonging to the organization *must* only be used in connection with the business activities/functions they are assigned and/or authorized.
- Every user is responsible for the preservation and correct use of the IT assets they have been assigned.
- Users shall maintain the assets assigned to them clean and free of accidents or improper use.
- Users must take special care to protect laptops and other portable assets from being stolen.
- All IT assets must be in locations with security access restrictions, environmental conditions, and layout according to the security classification and technical specifications of the assets. Lizu may consider purchasing a lockable steel cabinet to secure assets.
- Active laptops must be secured if left unattended, either manually locked or set to automatically self-lock after a maximum of 5 minutes of no activity.
- Access to organizational assets is forbidden for external/non-authorized personnel.
- The Executive Director has the sole responsibility for maintaining and upgrading configurations.
- Users must practice due diligence when installing applications and software.
- Portable equipment like laptops must remain in possession of the user as hand luggage when traveling by plane.
- Losses, theft, damages, tampering, or other incidents related to assets that compromise security must be reported as soon as possible to the Executive Director.
- Disposal of assets must be done according to specific procedures for the protection of information, with sensitive information being completely erased or physically destroyed as required.

2. Access Control Policy

2.1. Policy Definitions

- Systems hosting sensitive information must have up-to-date malware protection (ESET Security), a firewall where necessary, and be encrypted and appropriately patched.
- Systems handling valuable/sensitive work information must be protected with a password-based access control system.
- Systems handling confidential work information must use two-factor authentication-based access control system, if available.
- Users should not tamper with or evade access controls to gain greater access than they are assigned.

3. Physical Workspace Policy

3.1. Policy Definitions

- All unnecessary paper documents with confidential data must be destroyed using a shredder/scissors.
- Important documents, media, and small but valuable physical assets must be kept in a locked cabinet or drawer.

4. Password Control Policy

4.1. Scope

This policy includes all staff responsible for an account (or any form of access that supports or requires a password) on any system that belongs to Lizu, who have access to the Lizu network, or who store any non-public Lizu information. This policy applies to any person who is provided an account on Lizu's network or systems, including employees, guests, contractors, partners, and vendors.

4.2. Policy Definitions

- Systems handling valuable work information must be protected with a password-based access control system.
- Each login used to access organizational accounts and IT systems must have a strong, random, and unique password/passphrase that is at least 15 characters long.

- Passwords should be managed using **KeePassXC**, a secure and open-source password manager.
- Users are required to change their passwords immediately if a security incident or breach occurs on any platform where they use the same password. The website 'Have I Been Pwned?' (https://haveibeenpwned.com/) can be used to check if your email address or passwords have been compromised in known data breaches.
- Sharing passwords is forbidden. They should not be written down in notebooks, sticky notes, sent via email or exposed to public sight.
- Critical applications should use multi-factor authentication where possible.
- Staff managing organizational accounts must ensure the Executive Director is updated with current login credentials and that the IT Officer/ED has administrative rights on those accounts.
- Users should not check the "save/remember password" box when authenticating to web applications, nor use the same password for different systems/accounts.

5. Email Policy

5.1. Policy Definitions

- Assigned email addresses, mailbox storage, and transfer links must be used only for business purposes in the interest of Lizu.
- Use of organizational email resources for non-authorized advertising, external business, spam, personal service registration, political campaigns, and other uses unrelated to Lizu business is strictly forbidden.
- Users must not open unsolicited or suspicious-looking links and should check with the sender or refer to the Executive director or the designated Digital Security Champion when unsure.
- Organizational email resources may not be used to reveal confidential or sensitive information outside authorized recipients.
- Email resources may not be used to disseminate offensive, racist, obscene, or illegal content.
- Email identities must be protected by strong passwords.
- Scanning technologies for virus and malware must be in place on devices.
- Users must report security incidents as soon as possible.
- Use Google Drive for desktop, with organizational email accounts only, for secure storage and backups of sensitive email data.

6. Internet Policy

6.1. Policy Definitions

- Users should avoid accessing pornographic, hacking sites, and other risky sites using Lizu-assigned IT devices.
- Users must carefully check the address bar and browse only in HTTPS mode. Users may enable ‘HTTPS only mode’ in their browsers for safe browsing.

7. Antivirus Policy

7.1. Policy Definitions

- Computers and devices with access to Lizu’s cloud-based assets must have ESET Security antivirus client installed with real-time protection. Barring this, users must defer to the Executive Director or Digital Security Champion for advice on what antivirus to install and monitor the functionality of their antivirus.
- Antivirus must be set to automatically update virus definitions.
- Virus checks must be performed on materials from portable storage devices (USBs, external hard drives, etc.).

8. Mobile Device Management (MDM) Policy

8.1 Policy Definitions

- Sensitive information communicated via phone should use secure messaging apps such as Signal or Wire.
- Staff checking official emails on mobile phones should do so on a secure Internet connection, preferably with a VPN.
- Mobile devices used for work should have antivirus installed and be encrypted. The AV Test website (https://www.av-test.org/en/antivirus/mobile-devices/) may be used to determine a suitable antivirus.
- Mobile devices should have a screen lock mechanism.
- Mobile operating systems and apps must be kept up to date.
- Apps should be obtained from credible sources, with permissions checked before downloading.
- Organizationally assigned mobile devices should be configured for remote lock or wipe when lost or stolen.

9. Information Classification Policy

9.1. Policy Definitions

- Information owners must ensure the security of their information and supporting systems using VeraCrypt for encryption and locking mechanisms for devices.
- The Executive Director is responsible for ensuring the confidentiality, integrity, and availability of Lizu's assets.
- Breaches must be reported immediately, with appropriate countermeasures activated.
- Information in Lizu is classified as confidential, public, or private.
- Confidential information must have the highest level of security, with access limited to a few individuals.
- Public information can be shared as public records.
- Private information belongs to individuals responsible for its maintenance and backup.

10. Document Security, Storage & Backup Policy

10.1 Policy Definitions

- Sensitive information on computers should be kept in encrypted volumes using VeraCrypt.
- Users should perform regular backups, preferably every week, and enable automatic backups to cloud services.
- Physical backups should be encrypted on shared drives and external hard drives for business continuity and security.
- Sensitive information must be encrypted before uploading to cloud-based services.
- The Digital Security Champion is responsible for ensuring regular backups and testing backup sites.